SUMMARY OF THE AMENDMENTS

The present application contains forty-six (46) claims, numbered 35-42, 44-50 and 52-82.

Claims 43 and 51 have been cancelled.

Clerical amendments have been made to claims 39 and 44.

Claim 35 has been amended to include the features of former claim 43.

Claim 45 has been amended to include the features of former claim 51.

Claim 68 has been amended to include the features of former claim 43.

Claim 74 is new, and incorporates the features of former claims 35 and 44.

Claims 75-82 contain language identical to that of former claims 36-43.

It is believed that no new matter has been introduced by way of the present amendment.

REMARKS

Claim Rejections – 35 USC §102

On page 2 of the Office Action, the Examiner has rejected claims 35-73 under 35 USC 102(e) as being anticipated by Albert et al. (hereinafter referred to as Albert) U.S. patent application publication no. 20030056096A1.

CLAIM 35

It will be noted that claim 35 has been amended to include the features of former claim 43, which has been rejected on the same grounds as former claim 35[1]. The Applicant traverses the Examiner's rejection for the following reasons.

Amended claim 35 reads as follows:

> An authentication system, comprising:
>
> an access controller operable to communicate with a client via a first communication medium; and
>
> an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;
>
> wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.

Thus, in the claimed invention, a first key is delivered by an authentication server to a client and a second key is delivered by the server to an access controller. The keys are to be utilized in a verification protocol which, if met, allows the access controller to selectively pass to a computer (attached to the access controller) instructions received from the client. In addition, it is noted that the first key is delivered to the client only if a user operating the client authenticates that user's identity with the server. Therefore, authentication of the user is a pre-

[1] As a matter of clarification, it is assumed that paragraph 12 on page 4 of the Office Action pertains to claim 43 (not claim 44).

condition of the first key being delivered to the client. This allows only authenticated users to be entitled to communicate with the access controller.

Turning now to Albert, this reference basically teaches a method for authenticating network access credentials for users. Paragraphs [0059]-[0063], inter alia, describe a process whereby a client supplies a username and an encrypted password to a network access server (NAS). The NAS sends this information to a network decryption server (NDS). The NDS consults a database to determine, based on the username, which key it needs to use for decryption. It then decrypts the password to obtain a cleartext password. To determine whether this password is valid, the NDS sends the username and cleartext password to an AAA server, which then uses the username to determine the "official" password, and compares it to the cleartext password. Following this, if there is a match, "access to the internet or some other resource" is granted. Using this process, if it happens that the information traveling in association with the username anywhere between the client and the NDS (via the NAS) is sniffed or snooped, it will not reveal the user's password because it is encrypted.

Now, in the absence of detailed comments by the Examiner as to the relevance of Albert to former claim 43, it is difficult to ascertain how the Examiner has interpreted Albert. Two possibilities are addressed below.

If, on the one hand, the Examiner were to contend that Albert's disclosure is concerned with authentication of a client with the NAS/NDS, then it should be appreciated that Albert does not teach or suggest following authentication with a distribution of keys for use in a verification protocol. This is because, in Albert, access to the internet or some other resource would be granted during authentication, rendering such subsequent verification protocol useless.

On the other hand, if the Examiner were to contend that Albert's disclosure is concerned with implementation of a "verification protocol" involving a client, then it should be appreciated that Albert does not teach or suggest making the distribution of the client's key used in this verification conditional upon prior authentication of the client. This is because, in Albert, the

verification is itself the authentication, rendering such prior authentication redundant and/or meaningless.

Clearly, in neither case does Albert extend to the scenario where there is a decision made as to whether a client will or will not be given a key for communication with the NAS/NDS. Stated differently, Albert does not teach or suggest that in order for a first key (for utilization by a client in a verification protocol) to be distributed to the client by an authentication server, the user of the client needs to authenticate his or her identity with that server. It is thus apparent that at least one claimed feature is neither taught nor suggested by the cited art and, as such, it is respectfully submitted that the rejection of amended claim 35 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claim 35.

CLAIMS 36-42 and 44

Claims 36-42 and 44 are dependent on claim 35 and therefore incorporate by reference the limitations of claim 35. Thus, for the same reasons as those that apply to claim 35, it is respectfully submitted that the rejection of claims 36-42 and 44 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claims 36-42 and 44.

CLAIM 45

Amended claim 45 reads as follows:

> An access controller for intermediating communications between an interface and a computer and operable to store a second key complementary to a first key; said access controller operable to communicate with a client via said interface; said client operable to store said first key and to receive instructions from a user; said access controller operable to selectively pass said instructions to said computer if a verification protocol utilizing said keys is met;
>
> wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

Thus, in the claimed invention, an access controller participates in a verification protocol utilizing a first key stored by a client and a second key stored by the access controller. If the verification protocol is met, the access controller selectively passes (to a computer) instructions received from a user via the client. As part of the verification protocol, the client generates a random number that is encrypted (using the first key) and sent together with the (unencrypted) random number to the access controller. The access controller decrypts the encrypted random number using the second key and compares it to the received (unencrypted) random number. If there is a match, the verification protocol is said to have been met. Therefore, the access controller verifies whether the key that was supposed to have been used for encryption was actually used. Because there is an element of randomness in each verification, a successful verification provides a level of comfort that the commands are being issued from a legitimate source. There is no limitation on when the verification could be performed, namely it could be done once, periodicially or even for every packet.

Turning now to Albert, this reference basically teaches a method for authenticating network access credentials for users. Paragraphs [0059]-[0063], inter alia, describe a process whereby a client supplies a username and an encrypted password to a network access server (NAS). The NAS sends this information to a network decryption server (NDS). The NDS consults a database to determine, based on the username, which key it needs to use for decryption. It then decrypts the password to obtain a cleartext password. To determine whether this password is valid, the NDS sends the username and cleartext password to an AAA server, which then uses the username to determine the "official" password, and compares it to the cleartext password. Following this, if there is a match, "access to the internet or some other resource" is granted. Using this process, if it happens that the information traveling in association with the username anywhere between the client and the NDS (via the NAS) is sniffed or snooped, it will not reveal the user's password because it is encrypted.

However, Albert suffers from a slew of security-related problems. Consider firstly the case where the password is deemed invalid in Albert. This does not allow one to conclude whether the problem is with the password or with the encryption key, whereas transmitting the data in both encrypted and unencrypted form (as done in the claimed invention) would allow the dilemma to be resolved. Consider secondly the case where both the correct password and the

correct encryption key are used. If a malicious third party gains access to the encrypted password traveling between Albert's client and Albert's NAS/NDS, this one instance of "sniffing" the encrypted password is sufficient to give "access to the internet or some other resource", because the same encrypted password is transmitted each time. In contrast, the claimed invention provides an element of randomness that renders previously sniffed data obsolete to a malicious third party.

As such, Albert provides no possibility of comparing, on the basis of the received data (which is random), whether the password has been encrypted using an expected key. Stated differently, Albert does not teach or suggest a verification protocol whereby the client generates a random number that is encrypted (using the first key) and sent together with the (unencrypted) random number to the access controller, with the access controller subsequently decrypting the encrypted random number using the second key and comparing it to the received (unencrypted) random number. It is thus apparent that at least one claimed feature is neither taught nor suggested by the cited art and, as such, it is respectfully submitted that the rejection of amended claim 45 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claim 45.

CLAIMS 46-50 and 52-55

Claims 46-50 and 52-55 are dependent on claim 45 and therefore incorporate by reference the limitations of claim 45. Thus, for the same reasons as those that apply to claim 45, it is respectfully submitted that the rejection of claims 46-50 and 52-55 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claims 46-50 and 52-55.

CLAIMS 56-66 AND 70-73

On page 5, the Examiner states that "claims 45-73 do not teach or define any new limitations above claims 35-44, therefore, they are rejected for similar reasons." With all due respect, the Examiner is incorrect, at least insofar as claims 56-66 and 70-73 are concerned. Specifically, claims 56-66 deal with key updating, claims 70-71 include features found in claims 56-66 and

claims 72-73 deal with expiry of a verification protocol. In particular, it should therefore be appreciated that each of independent claims 56, 70 and 72 includes one or more features not recited by clams 35-44.

More specifically, claim 56 reads as follows (emphasis added):

> In an authentication server, a method of securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said method comprising:
>
> ***receiving a request from said access controller for an updated first key;***
>
> ***authenticating said request;***
>
> ***determining said updated first key and a second key corresponding to said updated first key; and***
>
> ***delivering said updated first key to said access controller.***

Claim 70 reads as follows (emphasis added):

> An authentication server for securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said authentication server comprising:
>
> ***means for receiving a request from said access controller for an updated first key;***
>
> ***means for authenticating said request;***
>
> ***means for determining said updated first key and a second key corresponding to said updated first key; and,***
>
> ***means for delivering said updated first key to said access controller.***

Claim 72 reads as follows (emphasis added):

> In an access controller for selectively passing instructions between a client and a computer if a verification protocol is met, a method of expiring said verification protocol, comprising:
>
> ***determining if a first preset period of time since said client disconnected from said access controller has elapsed;***
>
> ***determining if a second preset period of time since said verification protocol was updated has elapsed; and,***
>
> ***expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed.***

From a review of the above-emphasized features, it can be readily appreciated that the Examiner has not addressed the features of claims 56, 70 and 72 and, as such, it is respectfully submitted that a complete examination of the claims has not been affected, and therefore contravenes MPEP 707.07(g)[2].

It should also be pointed out that the additional features of claims 56, 70 and 72 are nowhere taught or suggested by the cited art and therefore the rejection of claims 56, 70 and 72 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claims 56, 70 and 72.

Claims 57-66, 71 and 73 are each dependent on one of claims 56, 70 or 72, and therefore incorporate by reference the limitations of the respective base claim. Thus, for the same reasons as those that apply to claims 56, 70 and 72, it is respectfully submitted that the rejection of claims 57-66, 71 and 73 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claims 57-66, 71 and 73.

CLAIM 67

Claim 67 reads as follows:

> A method of securing access between a client and a computer having an access controller intermediate said client and said computer, said method comprising:
>
> receiving an instruction at said client destined for said computer;
>
> generating a random number by said client;
>
> encrypting said random number by said client using a first key;
>
> delivering said random number, said encrypted random number and said instruction to said access controller;
>
> decrypting said encrypted random number using a second key by said access controller, said second key complementary to said first key;
>
> comparing said random number and said decrypted number;
>
> passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number; and,
>
> discarding said at least a portion if no match is found.

[2] "Piecemeal examination should be avoided as much as possible. The examiner ordinarily should reject each claim on all valid grounds available, [...]"

Thus, the claimed invention provides a method involving a client and an access controller. The client generates a random number that is encrypted (using a first key) and sent together with the (unencrypted) random number and an instruction for a computer. The access controller decrypts the encrypted random number using a second key and compares it to the received (unencrypted) random number. If there is a match, at least a portion of the instruction is passed to the computer. Therefore, the access controller verifies whether the key that was supposed to have been used for encryption was actually used. Because there is an element of randomness in each verification, a successful verification provides a level of comfort that the command was legitimately issued. There is no limitation on when the verification could be performed, namely it could be done once, periodicially or even for every packet.

It will be noted that claim 67 recites features similar to those of amended claim 45. Thus, based upon arguments consistent with those presented above in support of claim 45, it is respectfully submitted that claim 67 includes at least one feature not taught or suggested by the cited art. As such, it is respectfully submitted that the rejection of amended claim 67 under 35 USC 102 cannot stand, and the Examiner is therefore respectfully requested to withdraw the rejection of claim 67.

CLAIMS 68-69

Claim 68 reads as follows:

> An authentication server, comprising:
>
> an interface for communicating with a client and an access controller via a communication medium; and
>
> a processing unit operable to determine a first key for delivery to said client and a second key for delivery to said access controller, said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server; such that when said access controller and said client are connected, said access controller selectively passes instructions from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met.

It will be noted that claim 68 recites features similar to those of amended claim 35. Thus, based upon arguments consistent with those presented above in support of claim 35, it is

respectfully submitted that claim 68 includes at least one feature not taught or suggested by the cited art. As such, it is respectfully submitted that the rejection of amended claim 68 under 35 USC 102 cannot stand, and the Examiner is therefore respectfully requested to withdraw the rejection of claim 68.

Claim 69 is dependent on claim 68 and therefore incorporates by reference the limitations of claim 68. Thus, for the same reasons as those that apply to claim 68, it is respectfully submitted that the rejection of claim 69 under 35 USC 102 cannot stand. The Examiner is therefore respectfully requested to withdraw the rejection of claim 69.

Comments Regarding New Claims 74-82

New claim 74 reads as follows:

> An authentication system, comprising:
>
> an access controller operable to communicate with a client via a first communication medium; and
>
> an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;
>
> wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

Thus, in the claimed invention, a first key is delivered by an authentication server to a client and a second key is delivered by the server to an access controller. The keys are to be utilized in a verification protocol which, if met, allows the access controller to selectively pass to a computer (attached to the access controller) instructions received from the client. In addition, it is noted that delivery of the first key and the second key is effected only if the access controller transmits a preset second key that matches a record of this preset second key maintained by the authentication server. In this way, the access controller can be authenticated based on transmittal of an expected key (the preset second key), and successful

authentication of the access controller is a pre-condition of the first and second keys being delivered by the server. This ensures that communication will not take place with an access controller that is not authenticated.

Turning now to Albert, this reference basically teaches a method for authenticating network access credentials for users. Paragraphs [0059]-[0063], inter alia, describe a process whereby a client supplies a username and an encrypted password to a network access server (NAS). The NAS sends this information to a network decryption server (NDS). The NDS consults a database to determine, based on the username, which key it needs to use for decryption. It then decrypts the password to obtain a cleartext password. To determine whether this password is valid, the NDS sends the username and cleartext password to an AAA server, which then uses the username to determine the "official" password, and compares it to the cleartext password. Following this, if there is a match, "access to the internet or some other resource" is granted. Using this process, if it happens that the information traveling in association with the username anywhere between the client and the NDS (via the NAS) is sniffed or snooped, it will not reveal the user's password because it is encrypted.

It will be observed that authenticity of the NAS/NDS is never questioned in Albert. Stated differently, Albert does not teach or suggest that in order for first and second keys (for utilization by a client and an access controller in a verification protocol) to be distributed to the client and the access controller by an authentication server, the access controller needs to transmit a preset second key that matches a record of the preset second key maintained by that server. It is thus apparent that at least one claimed feature is neither taught nor suggested by the cited art and, as such, it is pre-emptively submitted that a rejection of new claim 74 under 35 USC 102 in view of Albert would be inappropriate.

Claims 75-82 are dependent on claim 74 and therefore incorporate by reference the limitations of claim 74. Thus, for the same reasons as those that apply to claim 74, it is pre-emptively submitted that a rejection of new claim 74 under 35 USC 102 in view of Albert would be inappropriate.

CONCLUSION

In view of the foregoing, Applicant is of the view that claims 35-42, 44-50 and 52-82 are in allowable form. Favourable reconsideration is requested. Early allowance of the Application is earnestly solicited.

If the application is not considered to be in full condition for allowance, for any reason, the Applicant respectfully requests the constructive assistance and suggestions of the Examiner in drafting one or more acceptable claims pursuant to MPEP 707.07(j) or in making constructive suggestions pursuant to MPEP 706.03 so that the application can be placed in allowable condition as soon as possible and without the need for further proceedings.

Respectfully submitted,

Date: October 1, 2007

Sanro Zlobec
Agent for Applicants
Reg. No. 52,535

SMART & BIGGAR
1000 De La Gauchetière Street West
Suite 3300
Montreal, Quebec H3B 4W5
CANADA
Telephone: (514) 954-1500
Facsimile: (514) 954-1396